CreateProcess-04

Fully qualify executable filename

Sean Barnum, Cigital, Inc. [vita[1]]

2007-03-20

Part "Original Cigital Coding Rule in XML"

Mime-type: text/xml, size: 7907 bytes

<table>
<tr><td><b>Attack Category</b></td><td>• Path spoofing or confusion problem</td></tr>
<tr><td><b>Vulnerability Category</b></td><td>• Process management
• Indeterminate File/Path</td></tr>
<tr><td><b>Software Context</b></td><td>• Process Management
• Threads and Processes</td></tr>
<tr><td><b>Location</b></td><td>• winbase.h</td></tr>
<tr><td><b>Description</b></td><td>When invoking CreateProcess() or related functions the executable filename should be fully qualified and include the file extension.
The CreateProcess function creates a new process and its primary thread. The new process runs the specified executable file in the security context of the calling process.
If the calling process is impersonating another user, the new process uses the token for the calling process, not the impersonation token. To run the new process in the security context of the user represented by the impersonation token, use the CreateProcessAsUser or CreateProcessWithLogonW function.
The lpApplicationName parameter can be NULL, in which case the executable name must be the first white space-delimited string in lpCommandLine. If the executable or path name has a space in it, there is a risk that a different executable could be run because of the way the function parses spaces.
This issue is reportedly fixed in Windows XP SP1, Windows Server 2003 and newer versions of Windows.</td></tr>
<tr><td><b>APIs</b></td><td><table>
<tr><th>FunctionName</th><th>Comments</th></tr>
<tr><td>CreateProcess</td><td></td></tr>
<tr><td>CreateProcessA</td><td></td></tr>
<tr><td>CreateProcessAsUser</td><td></td></tr>
</table></td></tr>
</table>

[1] http://buildsecurityin.us-cert.gov/bsi-rules/35-BSI.html (Barnum, Sean)

<table>
<tr><td></td><td><table>
<tr><td>CreateProcessAsUserA</td><td></td></tr>
<tr><td>CreateProcessAsUserW</td><td></td></tr>
<tr><td>CreateProcessW</td><td></td></tr>
<tr><td>CreateProcessWithLogon</td><td></td></tr>
<tr><td>CreateProcessWithLogonA</td><td></td></tr>
<tr><td>CreateProcessWithLogonW</td><td></td></tr>
</table></td></tr>
<tr><td><b>Method of Attack</b></td><td>An attacker could inject a Trojan horse executable into the system by placing a "tainted" executable in a location in the search path that is found before the intended executable.</td></tr>
<tr><td><b>Exception Criteria</b></td><td></td></tr>
<tr><td><b>Solutions</b></td><td><table>
<tr><th>Solution Applicability</th><th>Solution Description</th><th>Solution Efficacy</th></tr>
<tr><td>When creating a new process.</td><td>If lpApplicationName is not NULL, it should be fully qualified along with file extension (i.e. .exe, .com, .bat, .cmd). Otherwise, the current directory and .exe are assumed as location and extension.
Consider not passing NULL for lpApplicationName to avoid the function having to parse and determine the executable pathname from its runtime parameters. Otherwise, use quotations around the executable path in lpCommandLine, if</td><td>Effective.</td></tr>
</table></td></tr>
</table>

		lpApplicationName is NULL Don't specify NULL for the lpEnvironment parameter as the new process inherits the environment of the calling process. Only the minimum set of required environment variables should be passed to the child process. If the environment block pointed to by lpEnvironment contains Unicode characters, dwCreationFlags must include CREATE_UNICODE_ENVIRONMENT. Do not force lpStartup.lpDesktop to "winsta0\\default". If you do and the user is using Terminal Server, the application will run on the physical console, not the Terminal Server session that it is running from. Do not call CreateProcess from a DllMain function. This causes the application to stop	

	responding. (WinCE only)
Signature Details	BOOL CreateProcess(LPCTSTR lpApplicationName, LPTSTR lpCommandLine, LPSECURITY_ATTRIBUTES lpProcessAttributes, LPSECURITY_ATTRIBUTES lpThreadAttributes, BOOL bInheritHandles, DWORD dwCreationFlags, LPVOID lpEnvironment, LPCTSTR lpCurrentDirectory, LPSTARTUPINFO lpStartupInfo, LPPROCESS_INFORMATION lpProcessInformation); BOOL CreateProcessAsUser(HANDLE hToken, LPCTSTR lpApplicationName, LPTSTR lpCommandLine, LPSECURITY_ATTRIBUTES lpProcessAttributes, LPSECURITY_ATTRIBUTES lpThreadAttributes, BOOL bInheritHandles, DWORD dwCreationFlags, LPVOID lpEnvironment, LPCTSTR lpCurrentDirectory, LPSTARTUPINFO lpStartupInfo, LPPROCESS_INFORMATION lpProcessInformation); BOOL CreateProcessWithLogonW(LPCWSTR lpUsername, LPCWSTR lpDomain, LPCWSTR lpPassword, DWORD dwLogonFlags, LPCWSTR lpApplicationName, LPWSTR lpCommandLine, DWORD dwCreationFlags, LPVOID lpEnvironment, LPCWSTR lpCurrentDirectory, LPSTARTUPINFOW lpStartupInfo, LPPROCESS_INFORMATION lpProcessInfo);

Examples of Incorrect Code	`/* The following example is dangerous because the function will attempt to run "Program.exe", if it exists, instead of "MyApp.exe". */`
	
	`CreateProcessWithLogonW(..., L"C:\\Program Files\\MyApp -L -S", ...)`

<table>
<tr><td><b>Examples of Corrected Code</b></td><td><code>/* In the following, application name is properly quoted.
Note, however, that it would be even better to specify an non-null lpApplicationName */</code>

<code>CreateProcessWithLogonW(...,
L"\"C:\\Program Files\\MyApp.exe\"
-L -S", ...)</code></td></tr>
<tr><td><b>Source Reference</b></td><td>- http://msdn.microsoft.com/library/default.asp?url=/library/en-us/dnsecure/html/appsec.asp[2]</td></tr>
<tr><td><b>Recommended Resources</b></td><td>- MSDN reference for CreateProcess[3]</td></tr>
<tr><td><b>Discriminant Set</b></td><td><table>
<tr><td><b>Operating Systems</b></td><td>- Windows 98
- Windows Me
- Windows 2000
- Windows XP Home
- Windows XP Pro
- Win32</td></tr>
<tr><td><b>Languages</b></td><td>- C
- C++</td></tr>
</table></td></tr>
</table>

Cigital, Inc. Copyright

The Build Security In (BSI) portal is sponsored by the U.S. Department of Homeland Security (DHS), National Cyber Security Division. The Software Engineering Institute (SEI) develops and operates BSI. DHS funding supports the publishing of all site content.

[1] mailto:copyright@cigital.com